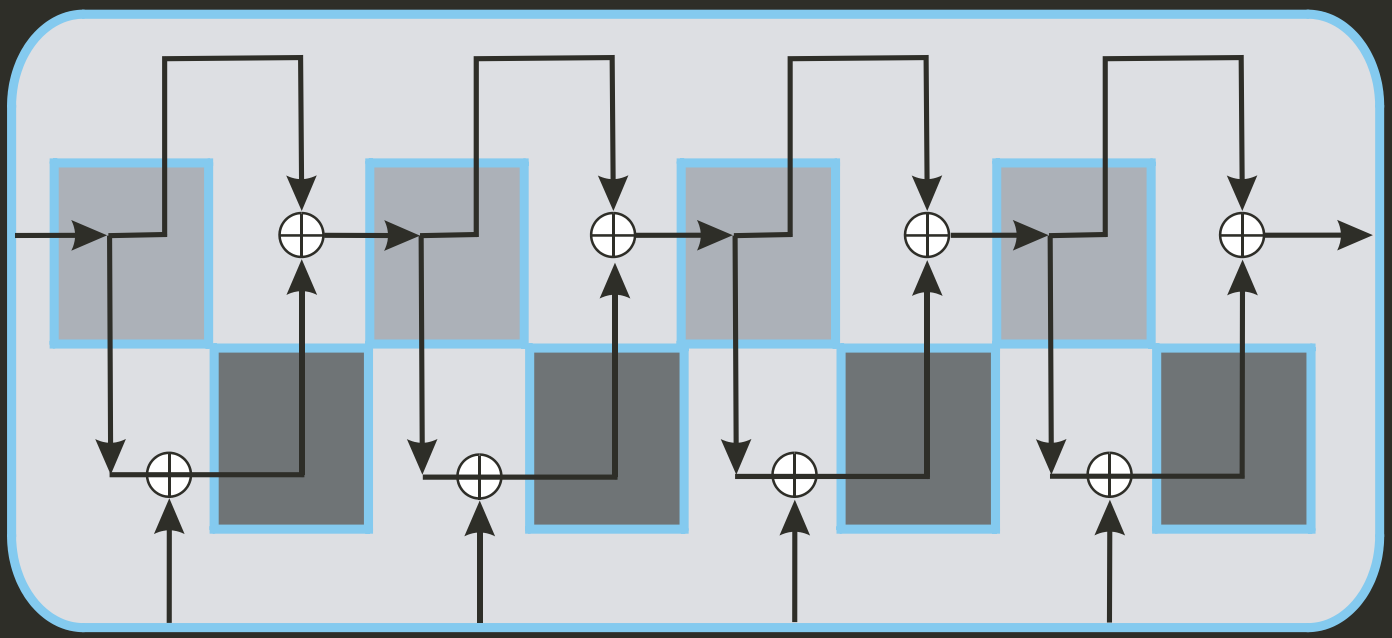
Journal of Research of the National Institute of Standards and Technology

May - June 2001, Vol. 106, No.3 ISSN 1044-677X

Advanced Encryption Standard Development Effort



NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Available online
http://www.nist.gov/jres

The National Institute of Standards and Technology was established in 1988 by Congress to ''assist industry in the development of technology . . . needed to improve product quality, to modernize manufacturing processes, to ensure product reliability . . . and to facilitate rapid commercialization . . . of products based on new scientific discoveries.''

NIST, originally founded as the National Bureau of Standards in 1901, works to strengthen U.S. industry's competitiveness; advance science and engineering; and improve public health, safety, and the environment. One of the agency's basic functions is to develop, maintain, and retain custody of the national standards of measurement, and provide the means and methods for comparing standards used in science, engineering, manufacturing, commerce, industry, and education with the standards adopted or recognized by the Federal Government.

As an agency of the U.S. Commerce Department's Technology Administration, NIST conducts basic and applied research in the physical sciences and engineering, and develops measurement techniques, test methods, standards, and related services. The Institute does generic and precompetitive work on new and advanced technologies. NIST's research facilities are located at Gaithersburg, MD 20899, and at Boulder, CO 80303. Major technical operating units and their principal activities are listed below. For more information contact the Publications and Program Inquiries Desk, 301-975-3058.

Office of the Director
- National Quality Program
- International and Academic Affairs

Technology Services
- Standards Services
- Technology Partnerships
- Measurement Services
- Information Services

Advanced Technology Program
- Economic Assessment
- Information Technology and Applications
- Chemistry and Life Sciences
- Materials and Manufacturing Technology
- Electronics and Photonics Technology

Manufacturing Extension Partnership Program
- Regional Programs
- National Programs
- Program Development

Electronics and Electrical Engineering Laboratory
- Microelectronics
- Law Enforcement Standards
- Electricity
- Semiconductor Electronics
- Radio-Frequency Technology[1]
- Electromagnetic Technology[1]
- Optoelectronics[1]

Materials Science and Engineering Laboratory
- Intelligent Processing of Materials
- Ceramics
- Materials Reliability[1]
- Polymers
- Metallurgy
- NIST Center for Neutron Research

Chemical Science and Technology Laboratory
- Biotechnology
- Physical and Chemical Properties[2]
- Analytical Chemistry
- Process Measurements
- Surface and Microanalysis Science

Physics Laboratory
- Electron and Optical Physics
- Atomic Physics
- Optical Technology
- Ionizing Radiation
- Time and Frequency[1]
- Quantum Physics[1]

Manufacturing Engineering Laboratory
- Precision Engineering
- Manufacturing Metrology
- Intelligent Systems
- Fabrication Technology
- Manufacturing Systems Integration

Building and Fire Research Laboratory
- Applied Economics
- Structures
- Building Materials
- Building Environment
- Fire Safety Engineering
- Fire Science

Information Technology Laboratory
- Mathematical and Computational Sciences[2]
- Advanced Network Technologies
- Computer Security
- Information Access
- Convergent Information Systems
- Information Services and Computing
- Software Diagnostics and Conformance Testing
- Statistical Engineering

[1] At Boulder, CO 80303.
[2] Some elements at Boulder, CO.

Journal of Research of the
National Institute of Standards and Technology

Volume 106 Number 3 May–June 2001

Available online
http://www.nist.gov/jres

U.S. Department of Commerce—**Donald L. Evans,** Secretary
Technology Administration—**Karen H. Brown,** Acting Under Secretary of Commerce for Technology
National Institute of Standards and Technology—**Karen H. Brown,** Acting Director

Cover: The cover illustration is symbolic of the Advanced Encryption Standard Development Effort at NIST. In 1997, NIST initiated a process to select a symmetric-key encryption algorithm to be used to protect sensitive (unclassified) Federal information. The research results and rationale for selection of the algorithm are documented in the article on p. 511 of this issue. Cover illustration arranged by C. Carey.

The *Journal of Research of the National Institute of Standards and Technology,* the flagship periodic publication of the national metrology institute of the United States, features advances in metrology and related fields of physical science, engineering, applied mathematics, statistics, and information technology that reflect the scientific and technical programs of the Institute. The *Journal* publishes papers on instrumentation for making accurate measurements, mathematical models of physical phenomena, including computational models, critical data, calibration techniques, well-characterized reference materials, and quality assurance programs that report the results of current NIST work in these areas. Occasionally, a Special Issue of the *Journal* is devoted to papers on a single topic. Also appearing on occasion are review articles and reports on conferences and workshops sponsored in whole or in part by NIST.

ISSN 1044-677X **Coden: JRITEF** **Library of Congress Catalog Card No.: 89-656121**

United States Government Printing Office, Washington: 2001

Volume 106, Number 3, May–June 2001
Journal of Research of the National Institute of Standards and Technology

Contents

Available online
http://www.nist.gov/jres

Articles

Conference Reports

News Briefs

Volume 106 Number 3, May–June 2001
Journal of Research of the National Institute of Standards and Technology